International Journal of Pure and Applied Mathematics
Volume 105 No. 3 2015, 325-338
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v105i3.1

PRIME WEIGHTED GRAPH IN CRYPTOGRAPHIC SYSTEM FOR SECURE COMMUNICATION

Shubham Agarwal[1] §, Anand Singh Uniyal[2]
[1,2]Department of Mathematics
M.B. (Govt.) P.G. College
Haldwani (U.K.), INDIA

Abstract: Cryptography is the study of techniques for ensuring the secrecy and authentication of the information. Public-key encryption schemes are secure only if the authenticity of the public-key is assured. Graph theory plays an important role in the field of cryptography for developing security schemes. In this paper we define the prime weighted graph and propose an efficient encryption scheme using prime weighted graph in cryptographic system for secure communication. Also, another aim is to design java program for the encryption/decryption algorithm.

AMS Subject Classification: 68R10, 94C15, 05C22
Key Words: cryptography, graph theory, prime weighted graph, security, encryption, decryption

1. Introduction

Cryptography was concerned totally with message encryption, i.e., the conversion of message from an intelligible form into unintelligible one and reverse again at the other end, rendering it unreadable by an unauthorized person without the knowledge of secret key (decryption key). In the modern age of technology cryptography is becoming a more and more central topic within computer sci-

Received: May 18, 2015

§Correspondence author

ence. As there is a need for more secure cryptographic schemes, the application of graph theory is going to increase for the development of secure encryption algorithms. R. Yadhu [1] have proposed a selective encryption mechanism using message specific key and spanning tree concept of graph theory. The mechanism provides protection of privacy in communication as it avoids the formation of self-loops and parallel edges and key is exchanged only among the authenticated persons only. Graph theory has a great contribution in the development of various encryption techniques. In this paper we propose a scheme for secure communication using prime weighted graph.

2. Cryptography

Cryptography [2] is the art and science of secure data communications over insecure channels. It is the study of method of sending messages in disguised form so that only the intended recipients can remove the disguise and interpret the message. Historically, the major consumers of cryptography were military and intelligence organizations. Today, however, cryptography is everywhere! Security mechanisms that rely on cryptography are an integral part of almost any computer system. Users rely on cryptography every time they access a secured website. Cryptographic methods are used to enforce access control in multi-user operating systems, and to prevent thieves from extracting trade secrets from stolen laptops. Software protection methods employ encryption, authentication, and other tools to prevent copying.

2.1. Cryptographic System

A cryptographic system [3] is any computer system that involves cryptography. Such systems include for instance, a system for secure electronic mail which might include methods for digital signatures, cryptographic hash functions, key management techniques, and so on. Cryptographic systems are made up of cryptographic primitives [4], and are usually rather complex. Because of this, breaking a cryptosystem is not restricted to breaking the underlying cryptographic algorithms; usually it is far easier to break the system as a whole.

2.2. Cryptanalysis

Cryptanalysis [5] refers to the art and science of analyzing information systems in order to study the hidden aspects of the systems. Cryptanalysis is used

to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key [6] is unknown.

3. Graph Theory

Graph theory is a branch of applied mathematics, which deals the problem with the help of graph. It is very easy to deal a problem graphically, as compare to theoretically. In mathematics and computer science, graph theory [7] is the study of graphs, which are mathematical structures used to model pair-wise relations between objects.

3.1. Graph

A graph [8] G = (V, E) consists of a set of objects V = v1, v2, v3, ... called vertices, and another set E = e1,e2, ... , whose elements are called edges, such that each edge ek is identify with an unordered pair (vi, vj) of vertices. The vertices associated with edge ek are called the end vertices of ek. The most common representation of a graph is by means of a diagram, in which the vertices are represented as points or nodes and each edge as a line segment joining its end vertices. Often this diagram itself is referred to as the graph. Figure 1 shows a graph G = (V, E) with vertex set V = a, b, c, d, e and the edge set E = e1, e2, e3, e4, e5, e6, e7, e8.

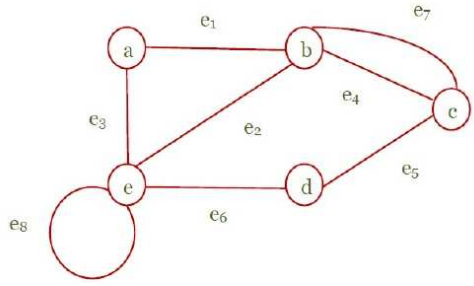

Figure 1: Graph

3.2. Simple Graph

A simple graph [9] G = (V, E) is consists of V, a non-empty set of vertices, and E, a set of unordered pairs of distinct elements of V called edges, having no self

loops (edges connected at both ends to the same vertex) and no parallel edges (more than one edge between any two different vertices). In a simple graph the edges of the graph form a set and each edge is a pair of distinct vertices. In a simple graph with n vertices, the degree of every vertex is at most (n-1). Figure 2 shows a simple graph.

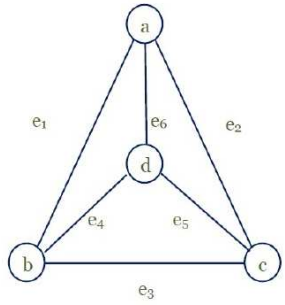

Figure 2: Simple Graph

3.3. Connected Graph

A graph G = (V, E) is said to be a connected graph [10] if there exists a path between every pair of vertices in G. Figure 3 shows a connected graph.

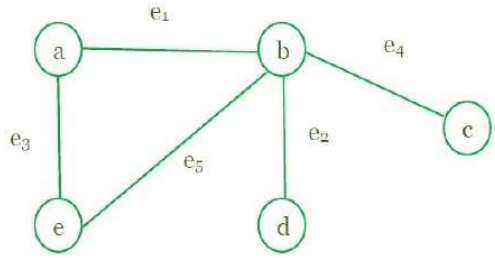

Figure 3: Connected Graph

3.4. Weighted Graph

A weighted graph [11] is a graph in which each edge (branch) is given a numerical weight. A weighted graph is therefore a special type of labeled graph in which the labels are numbers. Figure 4 shows a weighted graph.

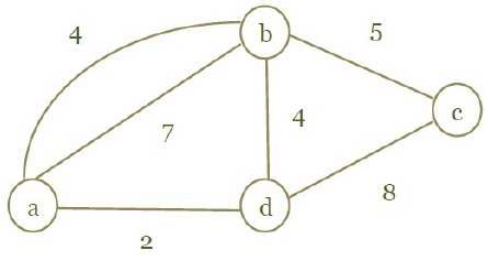

Figure 4: Weighted Graph

3.5. Prime Weighted Graph

A simple connected weighted graph G, in which the weight of each edge of the graph is a prime number, is called a prime weighted graph. Figure 5 shows a prime weighted graph.

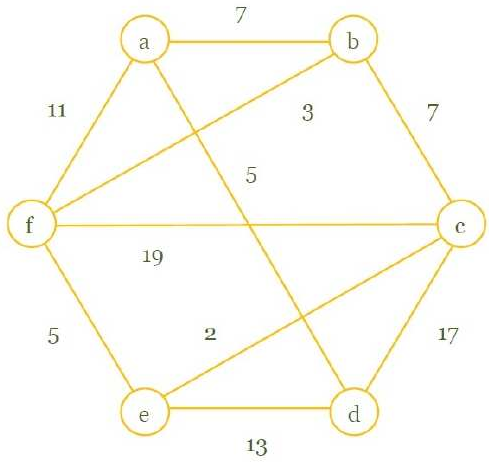

Figure 5: Prime Weighted Graph

4. Proposed Method

In this paper we aim to design a secure encryption / decryption algorithm using graph. In our proposed work the message will be encrypted in the form of the prime weighted graph. Since the graph is generated randomly, it is difficult

to understand that which edge of the graph should be selected first and then which edge will come next, without the knowledge of decryption key. In our proposed scheme, we have considered the simple graph because the existence of parallel edges and self loops will create uncertainty in the selection of the edges.

4.1. Encryption Chart

Use any normal encryption chart. Table 1 shows the ASCII value encryption chart.

4.2. Encryption Algorithm

Let the message be : IT IS SECRET.

Step-1: Assign the ASCII value to each character of the message using table 1. Table 2 shows the assignment of ASCII value to the characters.

Step-2: Add the length of the string in ASCII value corresponding to each character. Here the length of the string is 13. The addition of the length of the string in the ASCII value is shown in table 3.

Step-3: Assign a prime number for each numerical value getting after addition. if the value is a prime number then consider the number as it is and if the number is a composite number then add some value to it to make it a prime number just coming after it. So that all the characters are to be assigned a prime number as shown in table 4.

The encrypted string of prime numbers is shown in table 5.

Step-4: Draw a prime weighted graph randomly with the prime numbers assigned as the weights of the edges and the numbers of vertices are to be randomly selected.

Let us choose 7 vertices and randomly assign 13 prime numbers of the string to the 13 edges and draw a random prime weighted graph as shown in figure 6.

Step-5: Send this graph as the encrypted message.

Table 1: ASCII Value Encryption Chart

Decimal	Char	Decimal	Char	Decimal	Char	Decimal	Char
0	[NULL]	32	[SPACE]	64	@	96	`
1	[START OF HEADING]	33	!	65	A	97	a
2	[START OF TEXT]	34	"	66	B	98	b
3	[END OF TEXT]	35	#	67	C	99	c
4	[END OF TRANSMISSION]	36	$	68	D	100	d
5	[ENQUIRY]	37	%	69	E	101	e
6	[ACKNOWLEDGE]	38	&	70	F	102	f
7	[BELL]	39	'	71	G	103	g
8	[BACKSPACE]	40	(	72	H	104	h
9	[HORIZONTAL TAB]	41	)	73	I	105	i
10	[LINE FEED]	42	*	74	J	106	j
11	[VERTICAL TAB]	43	+	75	K	107	k
12	[FORM FEED]	44	,	76	L	108	l
13	[CARRIAGE RETURN]	45	-	77	M	109	m
14	[SHIFT OUT]	46	.	78	N	110	n
15	[SHIFT IN]	47	/	79	O	111	o
16	[DATA LINK ESCAPE]	48	0	80	P	112	p
17	[DEVICE CONTROL 1]	49	1	81	Q	113	q
18	[DEVICE CONTROL 2]	50	2	82	R	114	r
19	[DEVICE CONTROL 3]	51	3	83	S	115	s
20	[DEVICE CONTROL 4]	52	4	84	T	116	t
21	[NEGATIVE ACKNOWLEDGE]	53	5	85	U	117	u
22	[SYNCHRONOUS IDLE]	54	6	86	V	118	v
23	[END OF TRANS. BLOCK]	55	7	87	W	119	w
24	[CANCEL]	56	8	88	X	120	x
25	[END OF MEDIUM]	57	9	89	Y	121	y
26	[SUBTITUTE]	58	:	90	Z	122	z
27	[ESCAPE]	59	;	91	[	123	{
28	[FILE SEPARATOR]	60	<	92	\	124	|
29	[GROUP SEPARATOR]	61	=	93	]	125	}
30	[RECORD SEPARATOR]	62	>	94	^	126	~
31	[UNIT SEPARATOR]	63	?	95	_	127	[DEL]

Table 2: Assignment of ASCII Value to the Characters

Original Message	I	T		I	S		S	E	C	R	E	T	.
ASCII Value Corresponding to each character	73	84	32	73	83	32	83	69	67	82	69	84	46

Table 3: Addition of the Length of the String in the ASCII Value

Original Message	I	T		I	S		S	E	C	R	E	T	.
Number assigned to each character	73	84	32	73	83	32	83	69	67	82	69	84	46
Values after adding length of the string to ASCII value	86	97	45	86	96	45	96	82	80	95	82	97	59

Table 4: Assignment of a Prime Number to Each Character

Original Message	I	T		I	S		S	E	C	R	E	T	.
Number assigned to each character	73	84	32	73	83	32	83	69	67	82	69	84	46
Values after adding length of the string to ASCII value	86	97	45	86	96	45	96	82	80	95	82	97	59
Value to be added to make each number of the string prime	3	0	2	3	1	2	1	1	3	2	1	0	0
Prime number corresponding to each character	89	97	47	89	97	47	97	83	83	97	83	97	59

Table 5: Encrypted String of Prime Numbers

Prime numbers string	89	97	47	89	97	47	97	83	83	97	83	97	59

Java Program for Encrypting Original Message to the Sequence of Prime Numbers

```
import java.io.*;
class encryption
{
public static void main(String args[]) throws IOException
{
InputStreamReader reader=new InputStreamReader(System.in);
BufferedReader input=new BufferedReader(reader);
boolean res1,res2; String msg; int length,i,n; char ch;
System.out.println("Enter your message.....");
```

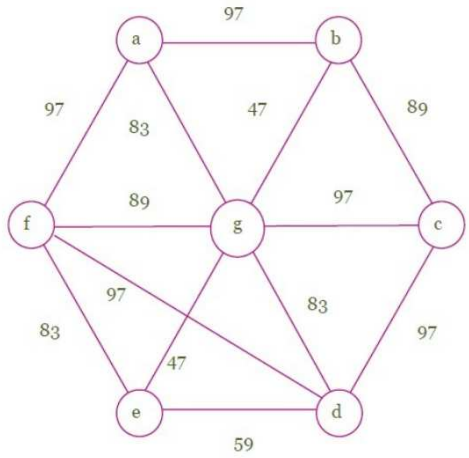

Figure 6: Prime Weighted Graph(Encrypted Message)

```
msg=input.readLine();
length=msg.length();
int nmsg[]=new int[length];
int pnmsg[]=new int[length];
int diff[]=new int[length];

    for(i=0;i<length;i++)
{
ch=msg.charAt(i); nmsg[i]=(int)ch; nmsg[i]=nmsg[i] +length;
}

    for(i=0;i<length;i++)
{
res1=isPrime(nmsg[i]);
if(res1==true)
pnmsg[i]=nmsg[i];
else
{
n=nmsg[i]+1;
while(true)
{
res2=isPrime(n);
if(res2==true)
```

```
{
pnmsg[i]=n; break;
}
n++;
}
}
}


    for(i=0;i<length;i++)
diff[i]=pnmsg[i]-nmsg[i];


    for(i=0;i<length;i++)
System.out.print(nmsg[i]+" ");
System.out.println();


    for(i=0;i<length;i++)
System.out.print(pnmsg[i]+" ");
System.out.println();


    for(i=0;i<length;i++)
System.out.print(diff[i]+" ");
}
static boolean isPrime(int n)
{
int i;
if(n==1 || n==0)
return false;
for(i=2;i<=n/2;i++)
{
if(n%i==0)
return false;
}
return true;
}
}
```

Table 6: Sequence of Edges (First Decryption Key)

Prime numbers string	89	97	47	89	97	47	97	83	83	97	83	97	59

Table 7: String of Prime Numbers

Second decryption key	3	0	2	3	1	2	1	1	3	2	1	0	0

Table 8: Second Decryption key

Prime numbers string	89	97	47	89	97	47	97	83	83	97	83	97	59
Second decryption key to be subtracted	3	0	2	3	1	2	1	1	3	2	1	0	0
Resultant string of numbers	86	97	45	86	96	45	96	82	80	95	82	97	59

4.3. Decryption Algorithm

For the decryption of the graph to the original message, first we must know the sequence of the edges which is to be considered. i.e, the first decryption key is the sequence of edges is shown in table 6.

Step-1: Write the weight of each edge corresponding to the sequence of edges to get the string of prime numbers as shown in table 7.

Step-2: Subtract the elements of second decryption key from the corresponding prime number. The second decryption key is shown in table 8.

The string of numbers after subtracting second decryption key is calculated in table 9.

Step-3: Now from this resultant string of numbers subtract the length of the string. Since in our message the length of the string is 13, therefore subtract 13 from each number of the resultant string. After subtraction the original string of numbers is shown in table 10.

Step-4: Now, using table 1 write the character corresponding to each num-

Table 9: String of Numbers after Subtracting Second Decryption Key

Resultant string of numbers	86	97	45	86	96	45	96	82	80	95	82	97	59
Length of the string	13	13	13	13	13	13	13	13	13	13	13	13	13
Original string of numbers after subtraction	73	84	32	73	83	32	83	69	67	82	69	84	46

Table 10: After Subtraction the Original String of Numbers

String of numbers	73	84	32	73	83	32	83	69	67	82	69	84	46
Corresponding character	I	T		I	S		S	E	C	R	E	T	.

Table 11: Character Corresponding to Each Number (ASCII value) of the String

String of numbers	73	84	32	73	83	32	83	69	67	82	69	84	46
Corresponding character	I	T		I	S		S	E	C	R	E	T	.

ber (ASCII value) of the string as shown in table 11 to get the original message.

Hence the original message is : IT IS SECRET.

Java Program for Decrypting Original Message from the Sequence of Prime Numbers

```
import java.io.*;
class decryption
{
public static void main(String args[]) throws IOException
{
InputStreamReader reader=new InputStreamReader(System.in);
BufferedReader input=new BufferedReader(reader);
int p[]=new int[100];
int d[]=new int[100];
```

```
int diff[]=new int[100];
int num,i,j,length;
System.out.println("Enter Length of string to be decrypted.....");
length=Integer.parseInt(input.readLine());

    for(i=0;i<length;i++)
{
System.out.println("Enter decrypted numbers one by one.....");
p[i]=Integer.parseInt(input.readLine());
}

    for(i=0;i<length;i++)
{
System.out.println("Enter keys one by one.....");
d[i]=Integer.parseInt(input.readLine());
}

    for(i=0;i<length;i++)
diff[i]=p[i]-d[i]-length;

    for(i=0;i<length;i++)
System.out.print((char)diff[i]+" ");
}
}
```

5. Conclusion

In the proposed method, while constructing the prime weighted graph, the selection of number of vertices and the assignment of edges is random, so it is hardly possible to predict for an unauthorized person that how many vertices should be chosen and which edge will come between which pair of vertices. Also it is very difficult to find the sequence of edges while decryption. Therefore the proposed algorithm is very useful for secure communication and has enormous potential to grow in future.

References

[1] Yadhu Ravinath , Vipul Mangla , Arkajit Bhattacharya , Peeyush Ohri, *Graph Theory Application in Selective Encryption Mechanism for Wireless Ad Hoc Network*, International Journal of Emerging Trends and Technology in Computer Science (IJETTCS) , ISSN 2278-6856, **Vol 2**, Issue 2, March - April (2013), page: 363-365.

[2] Song Y. Yan, *Computational Number Theory and Modern Cryptography*, John Wiley & Sons, USA (2012).

[3] Shubham Agarwal, Anand Singh Uniyal, *Elliptic Curves: An Efficient and Secure Encryption Scheme in Modern Cryptography*, International Journal of Advance Research in Science and Engineering (IJARSE), ISSN-2319-8354, **Vol. No.4**, Issue 03, March (2015), page: 134-143.

[4] http://en.wikipedia.org/wiki/Cryptographic primitive

[5] Cryptanalysis/Signals Analysis. Nsa.gov. 2009-01-15. Retrieved 2013-04-15.

[6] http://en.wikipedia.org/wiki/Key (cryptography)

[7] http://en.wikipedia.org/wiki/Graph theory

[8] Narsingh Deo, *Graph Theory with Applications to Engineering and Computer Science*, Prentice-Hall, Inc., (2004), ISBN: 9788120301450.

[9] Kenneth H. Rosen, *Discrete Mathematics and Its Applications*, McGraw Hill Education; 4th Revised edition (1 January 1999), ISBN: 978-0072899054.

[10] http://en.wikipedia.org/wiki/Connectivity (graph theory)

[11] http://mathworld.wolfram.com/WeightedGraph.html